ELSEVIER

Discrete Mathematics 167/168 (1997) 141–144

DISCRETE MATHEMATICS

Orthomorphisms of dihedral groups

Andrew Bowler

Department of Statistics, Birkbeck College, University of London, Malet Street, London WC1E 7HX, UK

Received 7 July 1995; revised 29 January 1996

Abstract

For $n \equiv 1, 5 \pmod 6$ it is shown that the dihedral group of order $4n$ admits a pair of orthogonal orthomorphisms.

1. Introduction

Let G be a finite group with identity element e. An *orthomorphism* of G is a permutation ϕ of the elements of G such that the mapping $x \mapsto x^{-1}\phi(x)$ is also a permutation of the elements of G. If ϕ is an orthomorphism and $\phi(e) = a$ for some $a \in G$ with $a \neq e$, then it is easy to check that the mapping ϕ' on G defined by $\phi'(x) = \phi(x)a^{-1}$ is an orthomorphism of G with $\phi'(e) = e$. Thus, for an orthomorphism ϕ of G we may assume that $\phi(e) = e$.

A related idea is that of a *complete mapping* of G. This is a permutation θ of the elements of G such that the mapping $x \mapsto x\theta(x)$ is also a permutation of the elements of G. It can be verified that ϕ is an orthomorphism of G if and only if the mapping $x \mapsto x^{-1}\phi(x)$ is a complete mapping of G. Because of the connection between the two ideas, many of the results regarding orthomorphisms of groups are couched in terms of complete mappings, in particular in the important papers [14,9].

Two orthomorphisms ϕ_1 and ϕ_2 of G are *orthogonal* if the mapping $x \mapsto (\phi_1(x))^{-1}\phi_2(x)$ is a permutation of the elements of G. The size of a largest set of pairwise orthogonal orthomorphisms of G will be denoted by $\omega(G)$. If G admits no orthomorphisms then we write $\omega(G) = 0$. A set of r pairwise orthogonal orthomorphisms of G can be used to construct $r + 1$ mutually orthogonal latin squares based on G. For details of this construction see [1] and [6]. Included in [2], [3] and [7] are sets of five mutually orthogonal latin squares of order 12 found by means of computer searches for orthomorphisms of $C_2 \times C_6$. For results on the existence of orthomorphisms of groups and their applications see [8].

PII S0012-365X(96)00222-1

2. Dihedral groups

The dihedral group D_{2n} of order $2n$ can be presented in the form

$$D_{2n} = \langle a, b : a^n = e,\ b^2 = (ab)^2 = e \rangle,$$

where e is the identity element. The elements of D_{2n} are then $e, a, \ldots, a^{n-1}$ together with $b, ab, \ldots, a^{n-1}b$. Also we have $ba^i = a^{-i}b$ for all integers i.

In [8, Problem 38] asks what can be said about $\omega(D_{2n})$. Before considering this we review some of the known results for dihedral groups. In [12,13], it is shown that any group of order $4m+2$ cannot admit an orthomorphism. This result is also a corollary of a more general result in [9]. It follows that $\omega(D_{2n}) = 0$ when n is odd. Thus, in looking for sets of pairwise orthogonal orthomorphisms of D_{2n} we need only consider the case when n is even. Using some of the results of [9] we have $\omega(D_{2n}) \geqslant 1$ when n is even. This result is also a consequence of the results in [11] which, for even n, can be used to construct an orthomorphism of D_{2n} in which all of the non-identity elements lie in the same cycle. Some results are known for small dihedral groups: it is easy to verify that $\omega(D_4) = 2$, both [4,10] give $\omega(D_8) = 1$ and [5] gives $\omega(D_{12}) = 2$.

In this paper we consider the general case of the dihedral group of order $4n$. In particular, we have the following result.

Theorem 2.1. *If* $\omega(\mathbb{Z}_n) \geqslant 2$, *then* $\omega(D_{4n}) \geqslant 2$.

Proof. Since $\omega(\mathbb{Z}_n) \geqslant 2$, there are at least two orthogonal orthomorphisms of $\mathbb{Z}_n$. Let ϕ_1 and ϕ_1' be orthogonal orthomorphisms of $\mathbb{Z}_n$. Define $\phi_2, \phi_2' : D_{4n} \to D_{4n}$ as follows:

x	a^{2i}	a^{2i+1}	$a^{2i}b$	$a^{2i+1}b$
$\phi_2(x)$	$a^{2\phi_1(i)}$	$a^{2\phi_1(i)}b$	$a^{2\phi_1(i)+1}b$	$a^{2\phi_1(i)+1}$
$\phi_2'(x)$	$a^{2\phi_1'(i)}$	$a^{2\phi_1'(i)+1}b$	$a^{2\phi_1'(i)+1}$	$a^{2\phi_1'(i)}b$

where $0 \leqslant i \leqslant n-1$.

We now verify that ϕ_2 and ϕ_2' are orthogonal orthomorphisms of D_{2n}. Since ϕ_1 and ϕ_1' are permutations of the elements of $\mathbb{Z}_n$, it is easy to check that ϕ_2 and ϕ_2' are permutations of the elements of D_{4n}.

For ϕ_2 we have

x	a^{2i}	a^{2i+1}	$a^{2i}b$	$a^{2i+1}b$
$x^{-1}\phi_2(x)$	$a^{-2i}a^{2\phi_1(i)}$	$a^{-2i-1}a^{2\phi_1(i)}b$	$a^{2i}ba^{2\phi_1(i)+1}b$	$a^{2i+1}ba^{2\phi_1(i)+1}$
	$= a^{2(\phi_1(i)-i)}$	$= a^{2(\phi_1(i)-i)-1}b$	$= a^{-2(\phi_1(i)-i)-1}$	$= a^{-2(\phi_1(i)-i)}b$

For ϕ_2' we have

x	a^{2i}	a^{2i+1}	$a^{2i}b$	$a^{2i+1}b$
$x^{-1}\phi_2'(x)$	$a^{2(\phi_1'(i)-i)}$	$a^{-2i-1}a^{2\phi_1'(i)+1}b$	$a^{2i}ba^{2\phi_1'(i)+1}$	$a^{2i+1}ba^{2\phi_1'(i)}b$
		$= a^{2(\phi_1'(i)-i)}b$	$= a^{-2(\phi_1'(i)-i)-1}b$	$= a^{-2(\phi_1'(i)-i)+1}$

Finally, for ϕ_2 and ϕ_2' we have

x	a^{2i}	a^{2i+1}
$(\phi_2(x))^{-1}\phi_2'(x)$	$a^{-2\phi_1(i)}a^{2\phi_1'(i)}$	$a^{2\phi_1(i)}ba^{2\phi_1'(i)+1}b$
	$= a^{2(\phi_1'(i)-\phi_1(i))}$	$= a^{-2(\phi_1'(i)-\phi_1(i))-1}$

x	$a^{2i}b$	$a^{2i+1}b$
$(\phi_2(x))^{-1}\phi_2'(x)$	$a^{2\phi_1(i)+1}ba^{2\phi_1'(i)+1}$	$a^{-2\phi_1(i)-1}a^{2\phi_1'(i)}b$
	$= a^{-2(\phi_1'(i)-\phi_1(i))}b$	$= a^{2(\phi_1'(i)-\phi_1(i))-1}b$

Thus, since ϕ_1 and ϕ_1' are orthogonal orthomorphisms of $\mathbb{Z}_n$, it follows that ϕ_2 and ϕ_2' are orthogonal orthomorphisms of D_{4n}. Hence $\omega(D_{2n}) \geqslant 2$. □

Note. Theorem 2.1 is relevant only when n is odd, since $\omega(\mathbb{Z}_n) = 0$ for even values of n.

Corollary 2.2. *If* $n \equiv 1, 5 \pmod 6$, *then* $\omega(D_{4n}) \geqslant 2$.

Proof. Let $\phi_1, \phi_1' : \mathbb{Z}_n \to \mathbb{Z}_n$ be the mappings defined by $\phi_1(x) = 2x$ and $\phi_1'(x) = 3x$. Since $n \equiv 1, 5 \pmod 6$ it follows that 2 and 3 are invertible elements of $\mathbb{Z}_n$ under multiplication and so ϕ_1 and ϕ_1' are permutations of the elements of $\mathbb{Z}_n$. Also $\phi_1(x) - x = x$, $\phi_1'(x) - x = 2x$ and $\phi_1'(x) - \phi_1(x) = x$. Thus, the mappings $x \mapsto \phi_1(x) - x$, $x \mapsto \phi_1'(x) - x$ and $x \mapsto \phi_1'(x) - \phi_1(x)$ are all permutations of $\mathbb{Z}_n$. Hence, ϕ_1 and ϕ_1' are orthogonal orthomorphisms of $\mathbb{Z}_n$, and the result follows from Theorem 2.1. □

The results of [15] can be used to show that $\omega(\mathbb{Z}_{15}) \geqslant 3$, $\omega(\mathbb{Z}_{21}) \geqslant 3$, $\omega(\mathbb{Z}_{33}) \geqslant 2$ and $\omega(\mathbb{Z}_{39}) \geqslant 2$, the details of which are given in [8]. These are the only values of $n \not\equiv 1, 5 \pmod 6$ for which it is known that $\omega(\mathbb{Z}_n) \geqslant 2$. Thus, using Theorem 2.1, we have the following result.

Corollary 2.3. *For* $n = 15$, 21, 33 *and* 39, $\omega(D_{4n}) \geqslant 2$.

Acknowledgements

The author would like to thank the referees for their helpful comments regarding the notation and terminology used in this paper, and for useful points regarding the references.

References

[1] D. Bedford, Orthomorphisms and near orthomorphisms of groups and orthogonal latin squares: a survey, Bull. Inst. Combin. Appl. 15 (1995) 13–33.

[2] R.C. Bose, I.M. Chakravarti and D.E. Knuth, On methods of constructing sets of mutually orthogonal latin squares using a computer I, Technometrics 2 (1960) 507–516.

[3] R.C. Bose, I.M. Chakravarti and D.E. Knuth, On methods of constructing sets of mutually orthogonal latin squares using a computer II, Technometrics 3 (1961) 111–117.
[4] L.Q. Chang and S.S. Tai, On the orthogonal relations among orthomorphisms of non-commutative groups of small orders, Acta Math. Sinica 14 (1964) 471–480. (Translation: Chinese Math. Acta 5 (1964) 506–515.)
[5] L.Q. Chang, K. Hsiang and S. Tai, Congruent mappings and congruence classes of orthomorphisms of groups, Acta Math. Sinica 14 (1964) 747–756. (Translation: Chinese Math. Acta 5 (1965) 141–152.)
[6] J. Dénes and A.D. Keedwell, Latin Squares and Their Applications (Akadémiai Kiadó, Budapest; Academic Press, New York; English Universities Press, London, 1974).
[7] A.L. Dulmage, D.M. Johnson and N.S. Mendelsohn, Orthomorphisms of groups and orthogonal latin squares I, Canad. J. Math. 13 (1961) 356–372.
[8] A.B. Evans, Orthomorphism graphs of groups, Lecture Notes in Mathematics, vol. 1535 (Springer, Berlin, 1992).
[9] M. Hall and L.J. Paige, Complete mappings of finite groups, Pacific J. Math. 5 (1955) 541–549.
[10] G. Grams and D. Jungnickel, Maximal difference matrices of order $\leqslant 10$, Discrete Math. 58 (1986) 199–203.
[11] A.D. Keedwell, On R-sequenceability and R_h-sequenceability of groups, Ann. Discrete Math. 18 (1983) 535–548.
[12] H.B. Mann, The construction of orthogonal latin squares, Ann. Math. Statist. 13 (1942) 418–423.
[13] H.B. Mann, On orthogonal latin squares, Bull. Amer. Math. Soc. 50 (1944) 249–257.
[14] L.J. Paige, Complete mappings of finite groups, Pacific J. Math. 1 (1951) 111–116.
[15] P.J. Schellenberg, G.H.J. Van Rees and S.A. Vanstone, Four pairwise orthogonal latin squares of order 15, Ars Combin. 6 (1978) 141–150.